RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: PART3-T01

Transforming Security Oversight with Forward-Looking Intelligence

Grant Bourzikas
Chief Security Officer, Cloudflare

Fred Kneip
Head of Platform, Diligent

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- **Security oversight evolution**
  Relevance of Security over the years
- **The context gap**
  When CISOs speak tech but boards need business
- **How we bridge the gap**
  Transforming raw data into actionable insight

Security oversight over the years

Security as a technology sub-function

Security oversight over the years

Standalone security department formed

Security as a technology sub-function

Security oversight over the years

- CISO/CSO role emerges and matures
- Standalone security department formed
- Security as a technology sub-function

Security oversight over the years

- Security as a board-level priority
- CISO/CSO role emerges and matures
- Standalone security department formed
- Security as a technology sub-function

Security oversight over the years

Security as a business enabler

Security as a board-level priority

CISO/CSO role emerges and matures

Standalone security department formed

Security as a technology sub-function

CISO & Board interactions today

- **Incident detection rate:** 99.7%
- **Security control coverage:** 92%
- **Mean time to patch:** 12.5 Days
- **Vulnerability count:** 237

CISO & Board interactions today

- **Incident detection rate:** 99.7%
- **Security control coverage:** 92%
- **Mean time to patch:** 12.5 Days
- **Vulnerability count:** 237

- ***Are we secure?***
- ***What's our risk?***
- ***What is the potential impact?***
- ***How do we compare to our peers?***

I provide detailed metrics and technical data in every report, but the board still asks me if we're secure. How can I answer that with a simple yes/no when security is a complex spectrum of risks and controls?"

- F500 CISO

Our CISO provides detailed security metrics, but I don't know what they mean to the overall company. It doesn't answer the question: Are we more or less secure than last quarter?"

- F500 Board Member

CISO & Board interactions today

CISO

- **Incident detection rate:** 99.7%
- **Security control coverage:** 92%
- **Mean time to patch:** 12.5 Days
- **Vulnerability count:** 237

The context gap

Board of Directors

- ***Are we secure?***
- ***What's our risk?***
- ***What is the potential impact?***
- ***How do we compare to our peers?***

What we are observing today

Engagement Gap

61% of Board Directors admit that Cyber Threats can derail a company's strategy and yet nearly **30% of Boards** operate without regular security input

Lagging Indicators

Almost all Security Board reporting today relies on **backward-looking data from disparate sources of data** that are hard to understand

Reporting Inconsistency

Lack of standardized reporting, similar to financial or operational data, is hampering the Board and CISO interactions in driving any active discussion or engagement

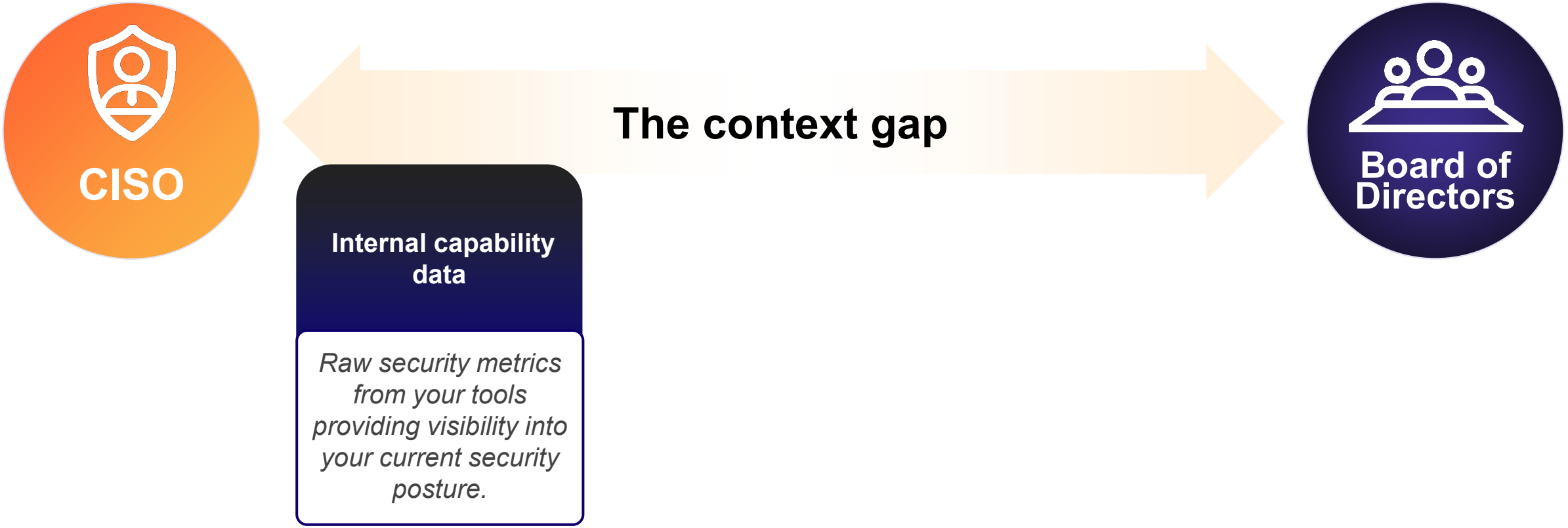
Expertise Shortage

75% of companies don't require Board cybersecurity education, leading to insufficient knowledge for meaningful security conversations

Source: Diligent Institute, 2025 What Directors Think Report

Bridging the context gap

Bridging the context gap


CISO
The context gap
Board of Directors
Internal capability data
Raw security metrics from your tools providing visibility into your current security posture.

Internal capability data

Security data sources available to CISOs today

- GRC platforms
- Security tools/Infrastructure
- Security data lake/Systems of record
- Third-party/Supply chain data
- Manual entry

Internal capability data

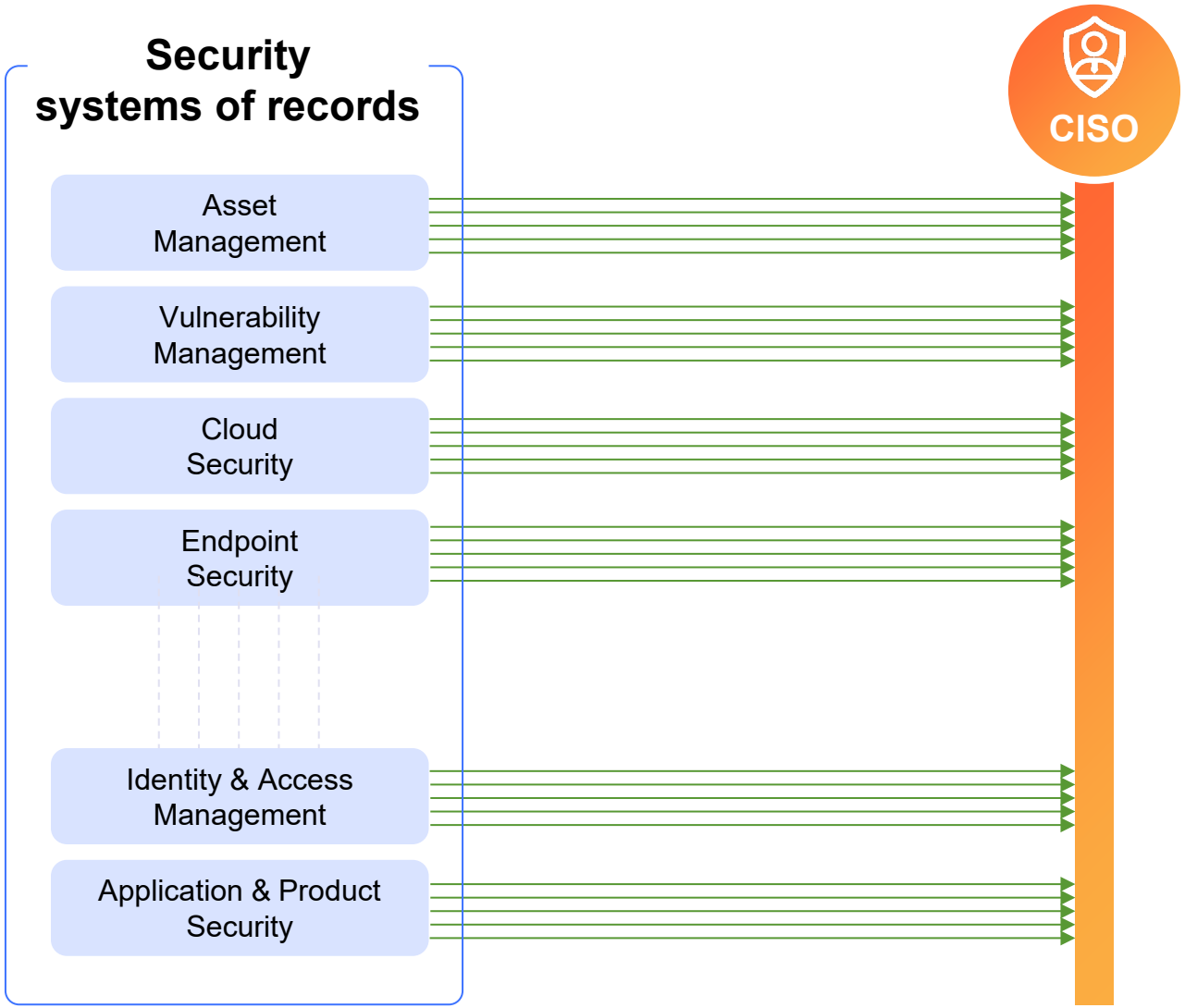
Security data sources available to CISOs today

- **GRC platforms**
- **Security tools/Infrastructure**
- **Security data lake/Systems of record**
- **Third-party/Supply chain data**
- **Manual entry**

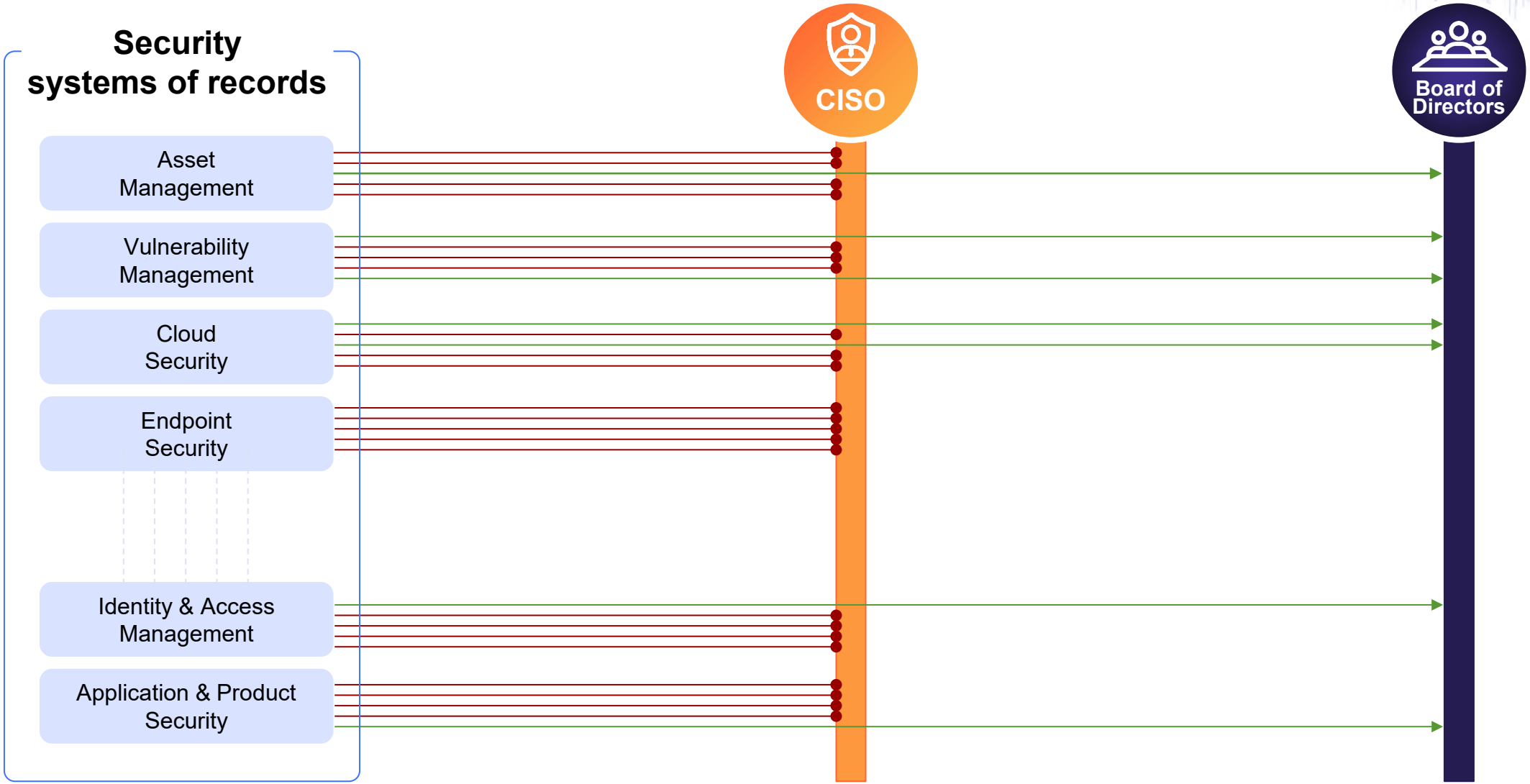
Blockers to unlocking the value of your internal data

1. **Siloed security data**
   Security tools operate independently without integration, creating disconnected views of your security posture
2. **Manual data collection**
   Reporting requires extensive manual effort to collect, format, and present security data
3. **Data integrity issues**
   Security data presented in reports often lacks traceability to its source, making verification difficult
4. **Fragmented narratives**
   Disconnected data points prevent telling a cohesive security risk story

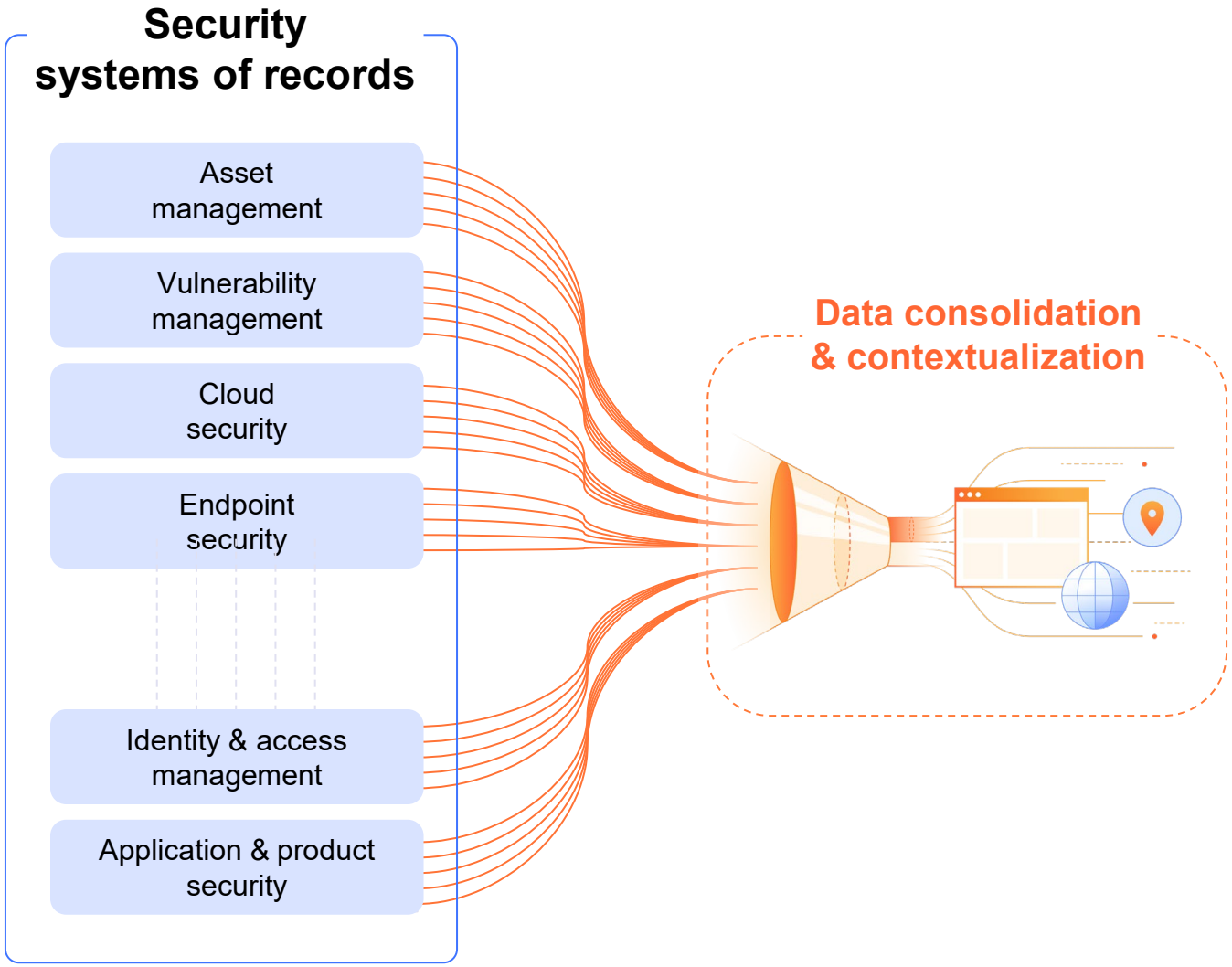
Reporting on internal capability data today



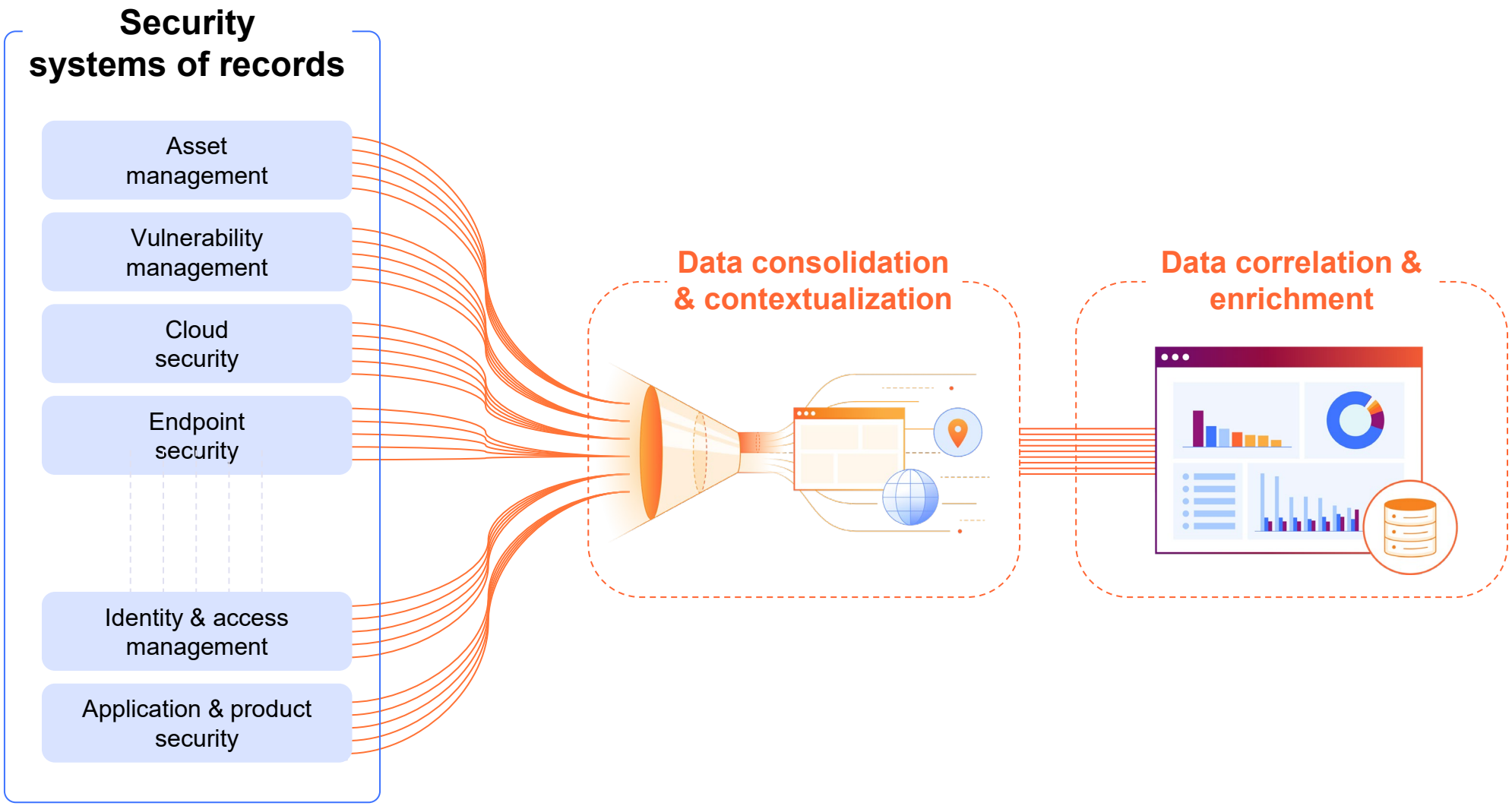
Reporting on internal capability data today



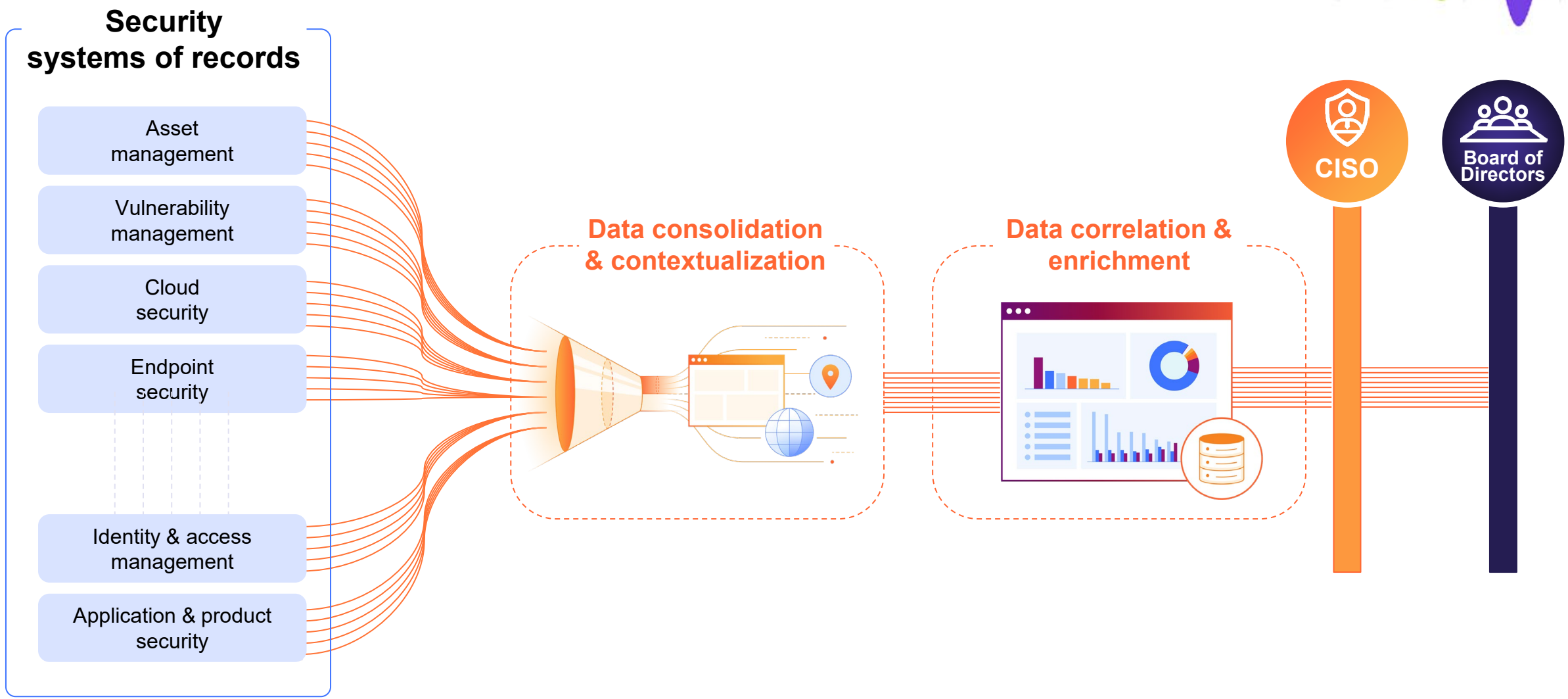
Unlocking the value of internal data



Unlocking the value of internal data



Unlocking the value of internal data

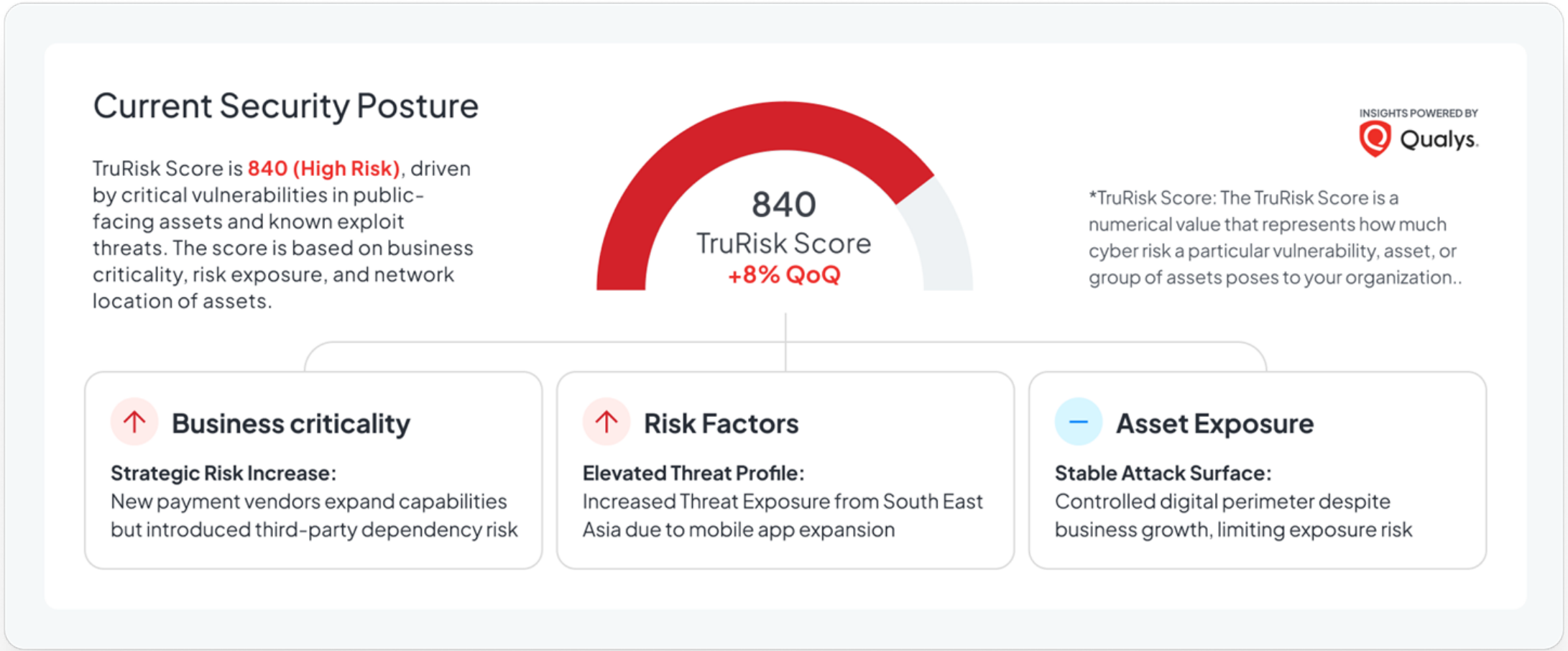


What board reporting looks like today

BEFORE:

What board reporting could look like tomorrow

AFTER:


Current Security Posture
TruRisk Score is 840 (High Risk), driven by critical vulnerabilities in public-facing assets and known exploit threats. The score is based on business criticality, risk exposure, and network location of assets.
840
TruRisk Score
+8% QoQ
INSIGHTS POWERED BY
Qualys.
*TruRisk Score: The TruRisk Score is a numerical value that represents how much cyber risk a particular vulnerability, asset, or group of assets poses to your organization..
Business criticality
Strategic Risk Increase:
New payment vendors expand capabilities but introduced third-party dependency risk
Risk Factors
Elevated Threat Profile:
Increased Threat Exposure from South East Asia due to mobile app expansion
Asset Exposure
Stable Attack Surface:
Controlled digital perimeter despite business growth, limiting exposure risk

What board reporting looks like today

BEFORE:

Board Security Report

March, 2025

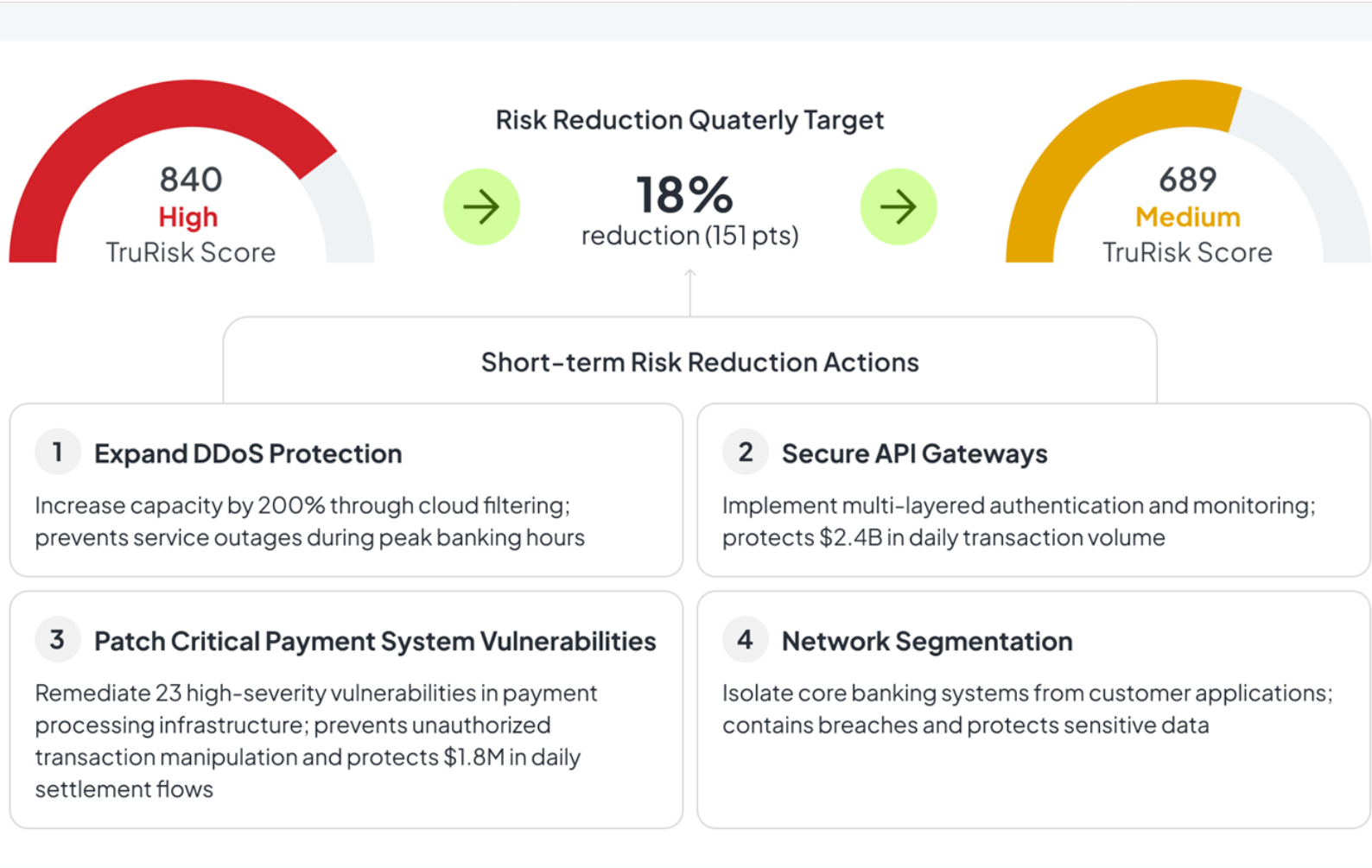
Security Program Maturity - NIST CSF

Security Initiatives

ID	Initiative Name	Status
1	**New Procurement Tool Implementation and Vendor Security Monitoring** Automates third-party security assessments and provides continuous monitoring of critical vendors, reducing risk exposure from supply chain compromises and ensuring regulatory compliance with vendor management requirements.	ON TRACK
2	**Network Segmentation** Creates secure boundaries between critical systems to prevent lateral movement by attackers, protecting customer data and core banking infrastructure by isolating systems based on security requirements and business function.	DELAYED
3	**Cloud Security Framework Implementation** Establishes comprehensive security controls for cloud environments, including access management, data protection, and compliance monitoring, enabling secure digital transformation while maintaining visibility across hybrid infrastructure.	ON TRACK
4	**Identity and Access Management Modernization** Implements zero-trust principles through advanced authentication methods and privilege management, reducing unauthorized access risks while improving user experience through streamlined access workflows.	DELAYED
5	**Security Awareness Training Program Enhancement** Develops customized security training based on role-specific risk profiles and uses simulated phishing campaigns to measure effectiveness, building a security-conscious culture to reduce human-factor vulnerabilities.	AT RISK

What board reporting could look like

AFTER:


Short-term Risk Reduction
840
High
TruRisk Score
Risk Reduction Quaterly Target
18%
reduction (151 pts)
689
Medium
TruRisk Score
Short-term Risk Reduction Actions
1 Expand DDoS Protection
Increase capacity by 200% through cloud filtering; prevents service outages during peak banking hours
2 Secure API Gateways
Implement multi-layered authentication and monitoring; protects $2.4B in daily transaction volume
3 Patch Critical Payment System Vulnerabilities
Remediate 23 high-severity vulnerabilities in payment processing infrastructure; prevents unauthorized transaction manipulation and protects $1.8M in daily settlement flows
4 Network Segmentation
Isolate core banking systems from customer applications; contains breaches and protects sensitive data

Bridging the context gap

CISO
The context gap
Internal capability data
+
External threat intelligence
Raw security metrics from your tools providing visibility into your current security posture.
Global threat insights providing context on the evolving risk landscape beyond your perimeter.
Board of Directors

External threat intelligence

Threat intelligence available to CISOs today

- Traditional threat feeds (IOCs, IPs, domains)
- Open-source intelligence (OSINT)
- Dark web monitoring
- Commercial threat intelligence platforms
- Industry-specific information sharing groups (ISACs)
- Vendor-specific security advisories
- Malware analysis reports

External threat intelligence

Threat intelligence available to CISOs today

- Traditional threat feeds (IOCs, IPs, domains)
- Open-source intelligence (OSINT)
- Dark web monitoring
- Commercial threat intelligence platforms
- Industry-specific information sharing groups (ISACs)
- Vendor-specific security advisories
- Malware analysis reports

Blockers to unlocking the value of your threat intel

1 Information Overload
Intelligence focuses on technical indicators and attack methods rather than translating into business risks that Boards can understand

2 Lack of Narratives
Intelligence data points aren't woven into compelling risk stories that demonstrate how threats could specifically impact business continuity or reputation

3 Predictive Limitations
Most intelligence describes what has already happened rather than providing forward-looking insights that help boards prepare for emerging threats

4 Capability Disconnect
Threat intelligence exists in isolation from the company's actual security capabilities, making it hard for boards to assess if the organization can effectively respond to identified threats

Threat intelligence today

Strategic threat intelligence

Too High-Level that limits any specificity to support decision making

Too detailed to gain any strategic intelligence, but value limited to SIEM/SecOps teams

Operational threat intelligence

Contextual threat insights

Strategic threat intelligence

Too High-Level that limits any specificity to support decision making

Contextual threat insights

Too detailed to gain any strategic intelligence, but value limited to SIEM/SecOps teams

Operational threat intelligence

Global visibility

- **Cross-industry threat monitoring:** Monitoring threats across diverse industry verticals to give early warning of emerging attack patterns
- **Geographic detection capabilities:** Geographic breadth that can enable detection of regional attack campaigns before they spread globally
- **Attack lifecycle visibility:** Visibility across the attack lifecycle to reveal threat actor tactics, techniques, and procedures (TTPs)

Intelligence specific to you

- **Industry and technology-specific threats:** Identifying which threats target your specific industry sector and technology stack
- **Strategic intent analysis:** Analyzing attack patterns to reveal strategic intent of threat actors
- **Threat Applicability:** Distinguishing between opportunistic threats and targeted campaigns

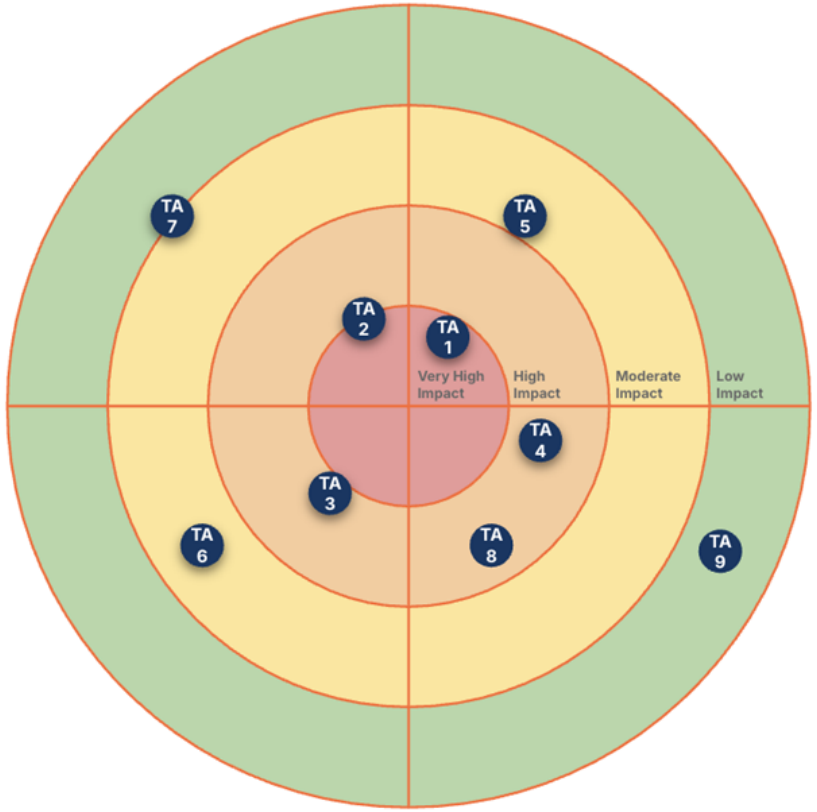
What board reporting looks like today

BEFORE:

Board Security Report

March, 2025

Threat Landscape Update



Threat Actors:

- **TA1 -** North Korean APT (Lazarus Group)
- **TA2 -** Russian State-Sponsored (APT29)
- **TA3 -** Financial Crime Syndicate (FIN7)
- **TA4 -** Chinese APT (APT41)
- **TA5 -** Ransomware Group (BlackCat)
- **TA6:** Various cybercriminal groups
- **TA7:** Opportunistic threat actors with limited capabilities
- **TA8:** Opportunistic threat actors with limited capabilities
- **TA9:** Opportunistic threat actors with limited capabilities

What board reporting could look like

AFTER:

Our Threat Landscape

GLOBAL CYBER THREAT INSIGHTS POWERED BY CLOUDFLARE

Malicious traffic distribution

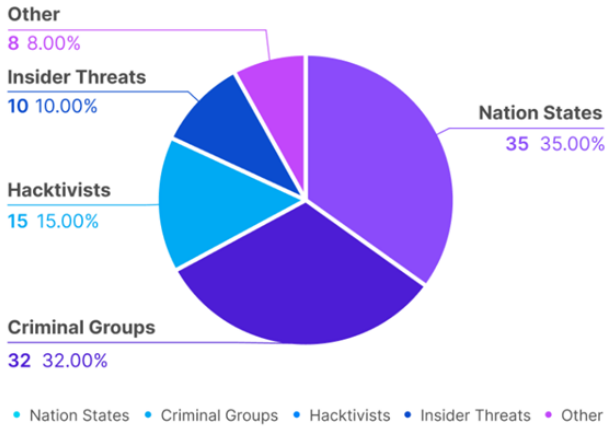
15% increase of malicious traffic

52% of malicious traffic originates from Southeast Asian countries, representing a **15% increase since our mobile banking app launch**.

*Malicious traffic: refers to network data (internet traffic) that has harmful intent or carries out cyberattacks.

Threat actor distribution

13% increase of cyber attacks



Nation states and criminal groups now account for 67% of attacks, up from 54% last quarter, showing an **accelerating shift toward sophisticated, targeted threats rather than opportunistic attacks.**

*Threat actor:which threat groups are responsible for attacks (e.g. cybercriminals vs nation-states)

What board reporting could look like

AFTER:

Current Industry Threats and Our Preparedness

01 Coordinated DDoS Attacks on Financial Institutions

Critical Protection Gaps

Potential Business Impact: These threats could result in online banking outages, payment service disruptions during high-volume periods

Current DDoS protection capacity insufficient for sophisticated attacks, limited by our network capacity

02 API Injection Attacks on Payment Processors

Basic Protection in Place

Potential Business Impact: These threats could result in potential transaction manipulation, unauthorized transfers, and service disruption

API security measures in place but third-party integration gaps exist

03 Supply Chain Compromise of Financial Software Vendors

Basic Protection in Place

Potential Business Impact: These threats could result in backdoor access to core banking systems, regulatory exposure, broad data compromise

Third-party risk management program requires enhancement

04 Advanced Banking Trojans Targeting Mobile Apps

Advanced Protection in Place

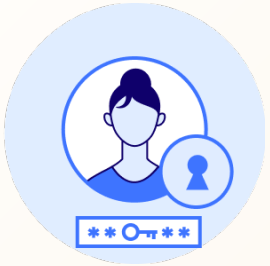
Potential Business Impact: These threats could result in potential data theft from customer mobile apps leading to fraud losses and repetitional harm.

Our app security controls and fraud monitoring would mitigate a majority of threat vectors

Bridging the context gap

CISO
The context gap
Internal capability data
+
External threat intelligence
+
Business context
Raw security metrics from your tools providing visibility into your current security posture.
Global threat insights providing context on the evolving risk landscape beyond your perimeter.
Translates technical metrics into business narratives that boards can internalize and act upon.
Board of Directors

Obstacles today with business context



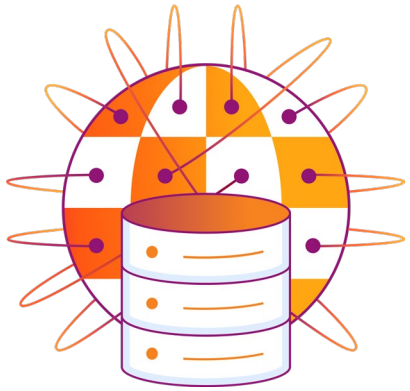
CISOs working in a silo with limited Business visibility

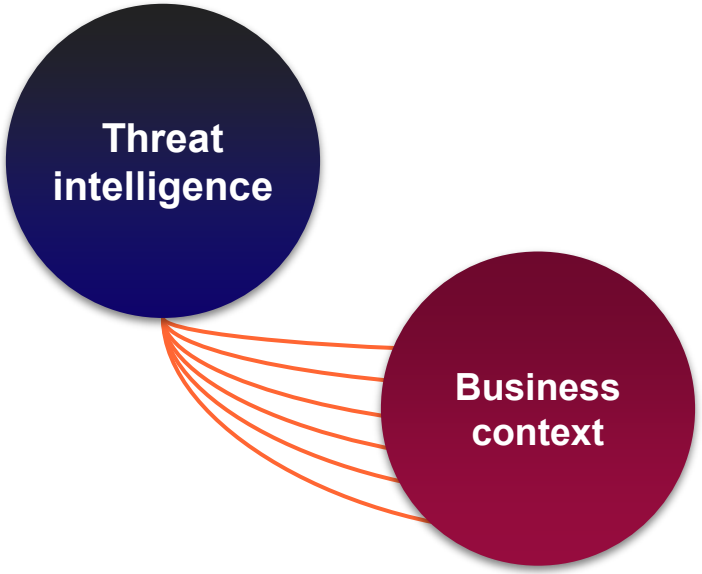
Security not at the table for business decisions

Security is viewed as a Technology problem

Leadership lack of Security knowledge

Business context as the translation layer



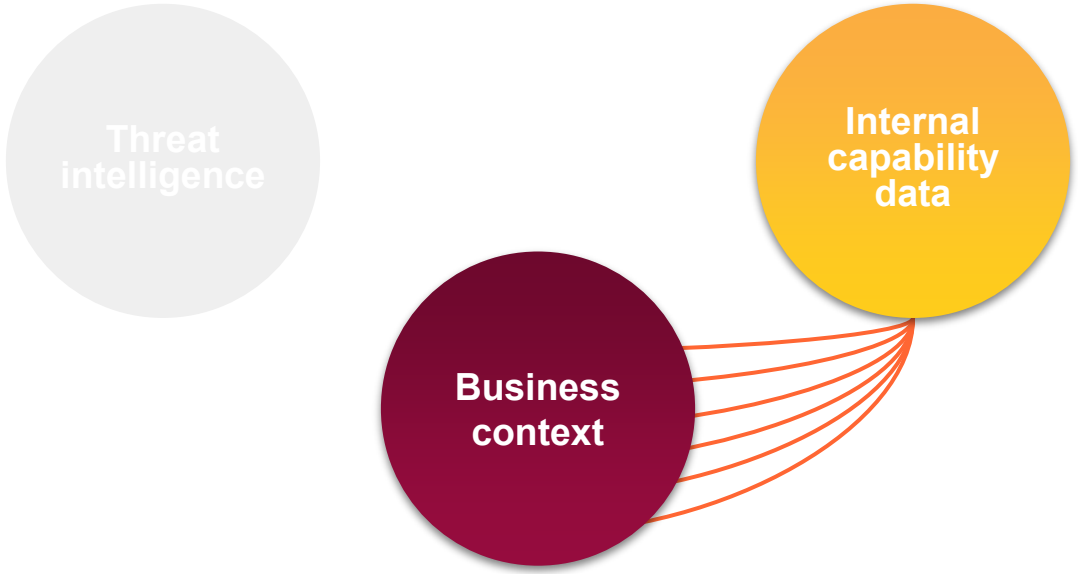


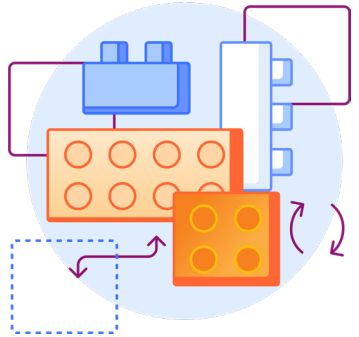
Internal capability data

FK

Correlate threat intelligence with business initiatives

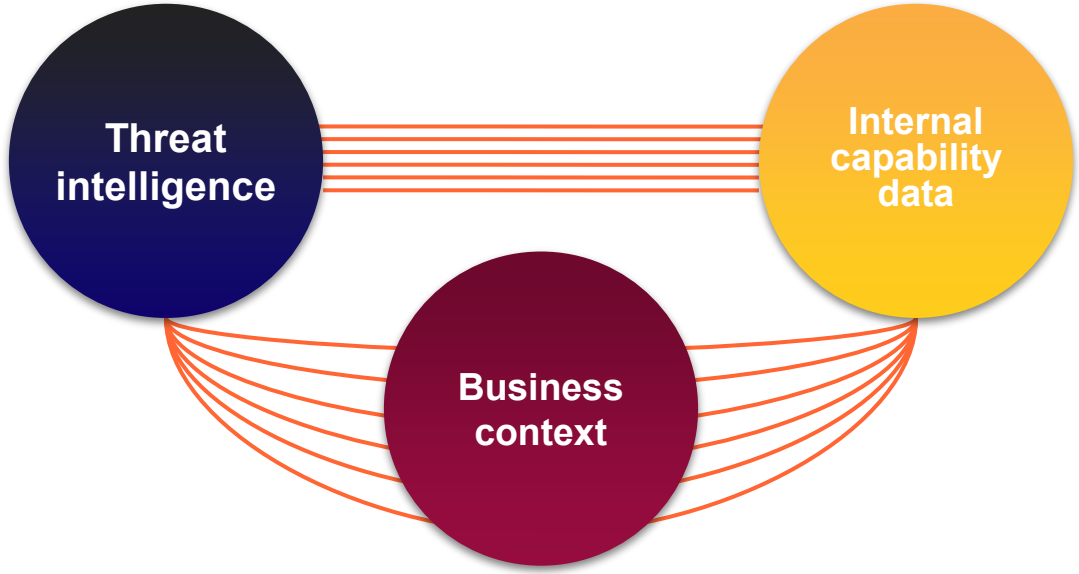
Business context as the translation layer

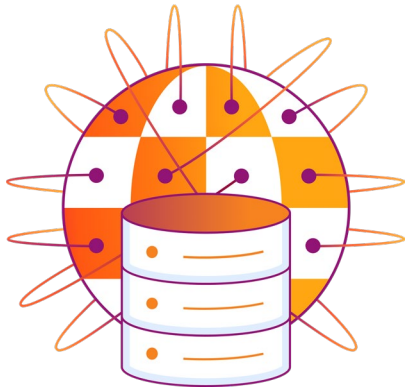




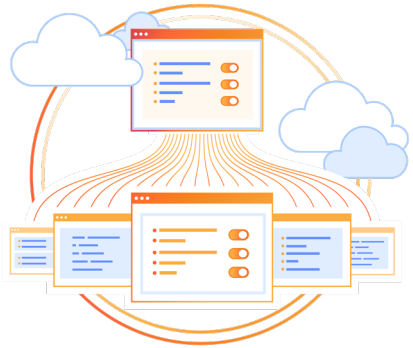
Quantify security's business contribution

Business context as the translation layer

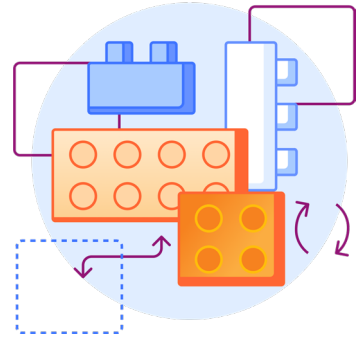




Correlate threat intelligence with business initiatives

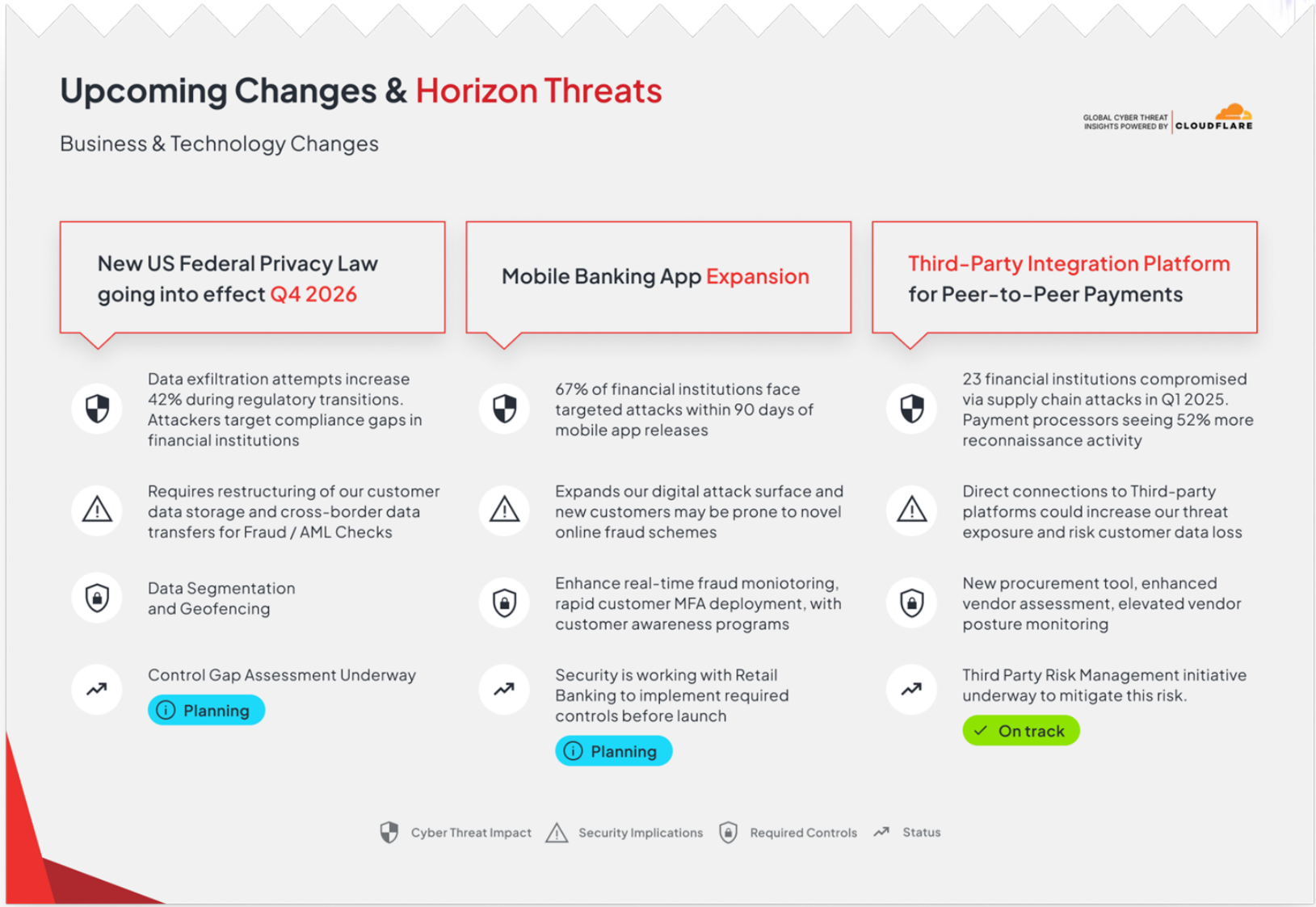


Deliver Integrated Security+Business reporting

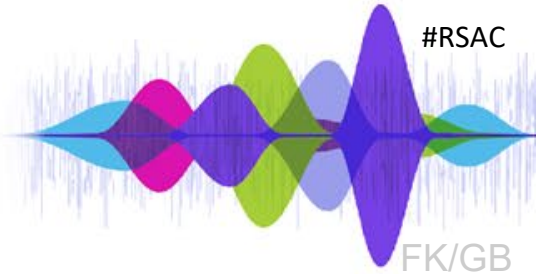


Quantify security's business contribution

What board reporting could look like


Upcoming Changes & Horizon Threats
Business & Technology Changes
GLOBAL CYBER THREAT INSIGHTS POWERED BY CLOUDFLARE
New US Federal Privacy Law going into effect Q4 2026
Mobile Banking App Expansion
Third-Party Integration Platform for Peer-to-Peer Payments
Data exfiltration attempts increase 42% during regulatory transitions. Attackers target compliance gaps in financial institutions
67% of financial institutions face targeted attacks within 90 days of mobile app releases
23 financial institutions compromised via supply chain attacks in Q1 2025. Payment processors seeing 52% more reconnaissance activity
Requires restructuring of our customer data storage and cross-border data transfers for Fraud / AML Checks
Expands our digital attack surface and new customers may be prone to novel online fraud schemes
Direct connections to Third-party platforms could increase our threat exposure and risk customer data loss
Data Segmentation and Geofencing
Enhance real-time fraud moniotoring, rapid customer MFA deployment, with customer awareness programs
New procurement tool, enhanced vendor assessment, elevated vendor posture monitoring
Control Gap Assessment Underway
Planning
Security is working with Retail Banking to implement required controls before launch
Planning
Third Party Risk Management initiative underway to mitigate this risk.
On track
Cyber Threat Impact
Security Implications
Required Controls
Status

Bridging the context gap

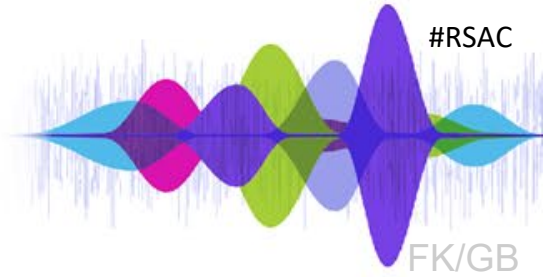


CISO

The Bridge

Board of Directors

Internal capability data	+	External threat intelligence	+	Business context
Raw security metrics from your tools providing visibility into your current security posture.		*Global threat insights providing context on the evolving risk landscape beyond your perimeter.*		*Translates technical metrics into business narratives that boards can internalize and act upon.*



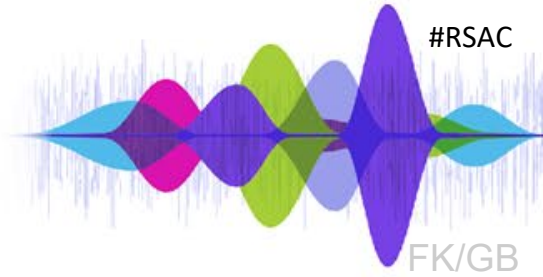
Summary

Key takeaways

1 Initiate Security + Business Alignment Sessions

Establish quarterly workshops where security and business leaders jointly assess how security capabilities enable specific business goals

Summary



Key takeaways

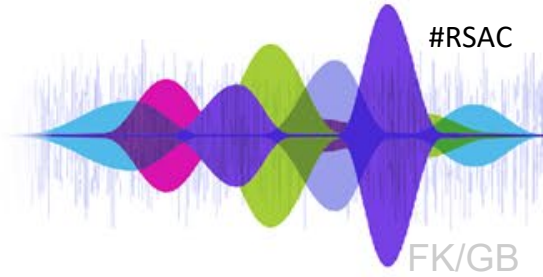
1 Initiate Security + Business Alignment Sessions

Establish quarterly workshops where security and business leaders jointly assess how security capabilities enable specific business goals

2 Integrate Threat Intelligence with Business Context

Map emerging threat patterns specifically to your organization's strategic initiatives, market entries, and growth opportunities

Summary



Key takeaways

1 Initiate Security + Business Alignment Sessions

Establish quarterly workshops where security and business leaders jointly assess how security capabilities enable specific business goals

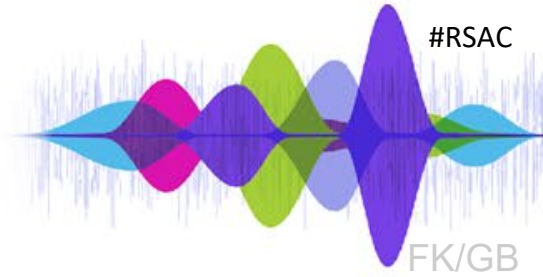
2 Integrate Threat Intelligence with Business Context

Map emerging threat patterns specifically to your organization's strategic initiatives, market entries, and growth opportunities

3 Translate Security to Business Value

Connect security metrics directly to revenue protection, competitive advantage, and customer trust metrics your Board already cares about

Summary



Key takeaways

1 Initiate Security + Business Alignment Sessions

Establish quarterly workshops where security and business leaders jointly assess how security capabilities enable specific business goals

2 Integrate Threat Intelligence with Business Context

Map emerging threat patterns specifically to your organization's strategic initiatives, market entries, and growth opportunities

3 Translate Security to Business Value

Connect security metrics directly to revenue protection, competitive advantage, and customer trust metrics your Board already cares about

4 Transform Reporting to drive Decisions

Replace technical dashboards with business impact narratives that enable clear prioritization and resource allocation choices

Build Your Bridge

RSAC 2025 Conference

Thank you